Abgeordnetenhaus BERLIN

Drucksache 19 / 24 686
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Stefan Ziller (GRÜNE)

vom 5. Januar 2026 (Eingang beim Abgeordnetenhaus am 5. Januar 2026)

zum Thema:

IT-Sicherheitsvorfälle in Berlin 2025

und **Antwort** vom 19. Januar 2026 (Eingang beim Abgeordnetenhaus am 20. Jan. 2026)

Der Regierende Bürgermeister von Berlin
Senatskanzlei

Herrn Abgeordneten Stefan Ziller (GRÜNE)
über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/24686
vom 5. Januar 2026
über IT-Sicherheitsvorfälle in Berlin 2025

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Wie viele IT-Sicherheitsvorfälle wurden 2025 durch Behörden und Institutionen der Berliner Verwaltung gem. § 23 II EGovGBln oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 1: Gemäß dem etablierten Meldeweg für IT-Sicherheitsvorfälle wurden im Jahr 2025 insgesamt acht Sicherheitsvorfälle durch Behörden und Institutionen der Berliner Verwaltung gemeldet.

2. Wie viele IT-Sicherheitsvorfälle wurden 2025 durch landeseigene Betriebe gem. § 23 II EGovGBln oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 2.: Im Zeitraum vom 01.01.2025 bis zum 31.12.2025 wurden dem Berlin-CERT zwei IT-Sicherheitsvorfälle durch landeseigene Betriebe gem. § 23 Abs. 2 EGovG Bln. gemeldet. Darüber hinaus erfolgte keine Meldung von IT-Sicherheitsvorfällen nach anderen Rechtsgrundlagen.

3. Wie viele der gemeldeten IT-Sicherheitsvorfälle wurden auch an die Berliner Beauftragte für Datenschutz und Informationsfreiheit nach § 51 BlnDSG oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 3.: Für die Bewertung eines IT-Sicherheitsvorfalls werden andere Kriterien herangezogen, als bei der Bewertung eines Datenschutzvorkommnisses. Betroffene Behörden und Einrichtungen melden in eigener Zuständigkeit ihre Datenschutzvorkommnisse an die Berliner Beauftragte für Datenschutz und Informationsfreiheit. Nicht jedes Datenschutzvorkommnis ist ein IT-Sicherheitsvorfall und umgekehrt. Eine gemeinsame Betrachtung liegt dem Senat nicht vor, da die Berliner Beauftragte für Datenschutz und Informationsfreiheit und der Landesbevollmächtigte für Informationssicherheit in jeweils eigener Zuständigkeit die ihnen gemäß maßgeblichen Kriterien gemeldeten Vorkommnisse bearbeiten.

4. Wie viele IT-Sicherheitsvorfälle wurden 2025 bekannt, die nicht durch die betroffenen Institutionen oder Unternehmen gemeldet wurden? Welche Konsequenzen hatte ein Ausbleiben von Meldungen?

Zu 4.: Es sind keine weiteren IT-Sicherheitsvorfälle bekannt.

5. Welche Empfehlungen hat das CERT des ITDZ in 2025 an betroffene Behörden, Institutionen und Unternehmen ausgesprochen? Wie viele der Empfehlungen wurden umgesetzt und in welchem Zeitraum? (Antwort bitte tabellarisch darstellen)

Zu 5.: Das Berlin-CERT hat jeweils die Koordinierung der Bearbeitung und Beseitigung der Sicherheitsvorfälle übernommen. Dabei wurden individuell, je nach Vorfall, die Sachlagen analysiert, und die ermittelten Bedrohungen durch geeignete Gegenmaßnahmen adressiert. Der Prozess der IT-Sicherheitsvorfallbearbeitung erfolgt dabei immer gemäß BSI Grundschutzkompendium DER 2.1 „Behandlung von Sicherheitsvorfällen“ in Verbindung mit BSI DER 2.3 „Bereinigung weitreichender Sicherheitsvorfälle“. Der Prozess beinhaltet unter anderem: Aufbau der Organisationsstruktur zur Behandlung von Sicherheitsvorfällen, Festlegung von Meldewegen, Eindämmung der Auswirkung, Einstufung von Sicherheitsvorfällen, Entscheidung und Umsetzung einer geeigneten Bereinigungsstrategie und Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Behebung. Der IT-Sicherheitsvorfall ist erst dann beendet, wenn ein ausreichender Bericht (inklusive Lessons Learned), erstellt wurde. Die Bearbeitung und Behebung der Sicherheitsvorfälle variierten zwischen 14 Tagen und 8 Monaten, je nach Umfang und notwendigen Maßnahmen.
Um keine zusätzlichen Bedrohungsvektoren zu geben, wird zur Risikominimierung hier auf eine detaillierte Aufstellung der einzelnen Angriffe verzichtet.

6. Welche erfolgreichen Angriffe gab es in 2025 auf die Behörden, Institutionen der Berliner Verwaltung und landeseigenen Betriebe und welche Konsequenzen wurden daraus gezogen? (Antwort bitte tabellarisch darstellen)

Zu 6.: Je nach Art und Schwere des IT-Sicherheitsvorfalls mussten unterschiedliche Maßnahmen (als Konsequenz) zu seiner erfolgreichen Beseitigung ergriffen werden.
Dazu gehörten unter anderem:

- Systemhärtung,
- Aufbau sicherer Kommunikationskanäle,
- Eindämmung betroffener Systeme / Isolierung betroffener Netzabschnitte,
- Hard- und Softwaretausch,
- Schließen des initialen Einfallsvektor,
- Sperrung und Änderung von Zugangsdaten und kryptografischen Algorithmen,
- Neukonzeptionierung und Aufbau der Systeminfrastruktur,
- Bewertung und Neugestaltung von Prozessen und
- Migration der betroffenen Behörden in die Umgebung des gesicherten Berliner Landesnetzes.

Um keine zusätzlichen Bedrohungsvektoren zu geben, wird zur Risikominimierung hier auf eine detaillierte Aufstellung der einzelnen Angriffe verzichtet.

Berlin, den 19. Januar 2026

Der Regierende Bürgermeister von Berlin
In Vertretung

Martina Klement
Staatssekretärin für Digitalisierung
und Verwaltungsmodernisierung / CDO